Customer Number 22,852
Attorney Docket No. 06753.0439

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors: Takahiro ABE et al.

Serial No.: 09/822,459 — Group Art Unit: 2131

Filed: April 2, 2001

For: STREAM ENCIPHERING METHOD, DECIPHERING METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

CLAIM FOR PRIORITY

Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 2000-100909, for the above identified United States Patent Application.

In support of applicants claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: October 30, 2001

By: David W. Hill
David W. Hill
Reg. No. 31,744

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

#4

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: April 3, 2000

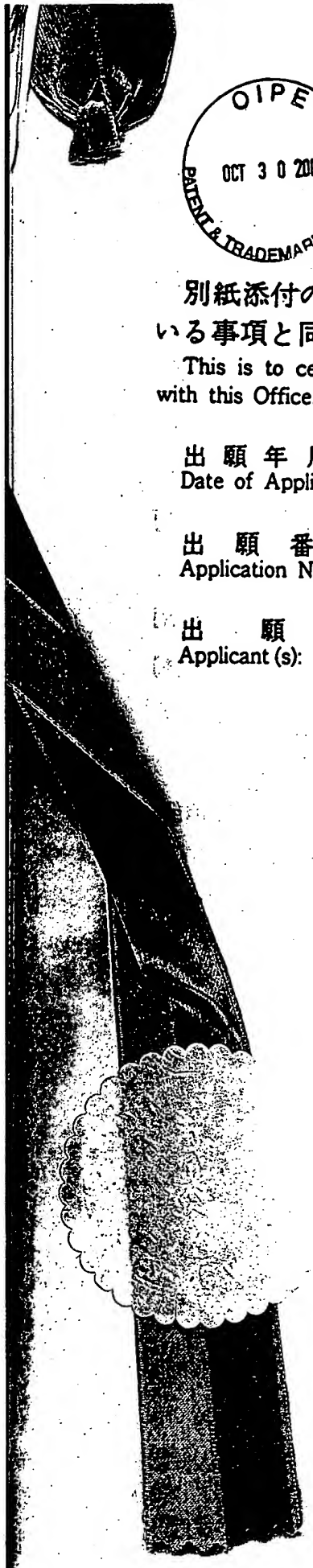
Application Number: Patent Application
No. 2000-100909

Applicant(s): YAZAKI CORPORATION
Micro-Technology Corporation

March 2, 2001

Commissioner,
Patent Office Kouzou OIKAWA

Number of Certificate: 2001-3014263



#4

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

09/822459

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月　３日

出願番号
Application Number: 特願２０００－１００９０９

出願人
Applicant (s): 矢崎総業株式会社
マイクロテクノロジ株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　３月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１４２６３

【書類名】　特許願

【整理番号】　YZK-4913

【提出日】　平成12年 4月 3日

【あて先】　特許庁長官殿

【国際特許分類】　H03B 29/00

G09C 1/00

H01L 29/78

【発明の名称】　ストリーム暗号化方法、復号方法、及び暗号通信システム

【請求項の数】　3

【発明者】

【住所又は居所】　静岡県裾野市御宿１５００　矢崎総業株式会社内

【氏名】　阿部　考浩

【発明者】

【住所又は居所】　神奈川県横浜市旭区白根５丁目４５番１２号

【氏名】　庄野　克房

【特許出願人】

【識別番号】　000006895

【氏名又は名称】　矢崎総業株式会社

【代表者】　矢崎　裕彦

【特許出願人】

【識別番号】　591235810

【氏名又は名称】　マイクロテクノロジ株式会社

【代表者】　山田　敬

【代理人】

【識別番号】　100083806

【弁理士】

【氏名又は名称】　三好　秀和

【電話番号】　03-3504-3075

【選任した代理人】

【識別番号】　100068342

【弁理士】

【氏名又は名称】　三好　保男

【選任した代理人】

【識別番号】　100100712

【弁理士】

【氏名又は名称】　岩▲崎▼　幸邦

【選任した代理人】

【識別番号】　100087365

【弁理士】

【氏名又は名称】　栗原　彰

【選任した代理人】

【識別番号】　100079946

【弁理士】

【氏名又は名称】　横屋　趙夫

【選任した代理人】

【識別番号】　100100929

【弁理士】

【氏名又は名称】　川又　澄雄

【選任した代理人】

【識別番号】　100095500

【弁理士】

【氏名又は名称】　伊藤　正和

【選任した代理人】

【識別番号】　100101247

【弁理士】

【氏名又は名称】　高橋　俊一

【選任した代理人】

【識別番号】　100098327

【弁理士】

【氏名又は名称】　高松　俊雄

【手数料の表示】

【予納台帳番号】　001982

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708734

【包括委任状番号】　9902582

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ストリーム暗号化方法、復号方法、及び暗号通信システム

【特許請求の範囲】

【請求項１】　秘匿対象となる平文コードに対し、ＰＮ信号との間で排他的論理和演算を行わせることにより、暗号コードを生成するストリーム暗号化方法において、

前記ＰＮ信号の周期として、前記平文コードの処理基本単位とは相容れない周期を採用したことを特徴とするストリーム暗号化方法。

【請求項２】　請求項１に記載のストリーム暗号化方法を用いて暗号化された暗号コードを平文コードに復元する復号方法において、

前記暗号コードに対し、前記ＰＮ信号と同一のＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、前記暗号コードをもとの平文コードに復元することを特徴とする復号方法。

【請求項３】　送信側と受信側との間で情報の暗号通信を遂行し得るように構成された暗号通信システムにおいて、

前記送信側は、

秘匿対象となる平文コードを処理基本単位毎に記憶する平文記憶手段と、

前記平文コードの処理基本単位とは相容れない周期となるＰＮ信号を記憶する送信側ＰＮ信号記憶手段と、

前記平文記憶手段に記憶されている平文コードに対し、前記送信側ＰＮ信号記憶手段に記憶されているＰＮ信号との間で排他的論理和演算を行わせることにより、暗号コードを生成する暗号化手段と、

この暗号化手段で生成した暗号コードを受信側宛に送信する送信手段と、

を備える一方、

前記受信側は、

前記送信手段から送信されてきた暗号コードを受信する受信手段と、

この受信手段で受信した暗号コードを処理基本単位毎に記憶する暗号文記憶手段と、

前記送信側ＰＮ信号記憶手段に記憶されているＰＮ信号と同一のＰＮ信号を記

憶する受信側ＰＮ信号記憶手段と、

前記暗号文記憶手段に記憶されている暗号コードに対し、前記受信側ＰＮ信号記憶手段に記憶されているＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、前記暗号コードをもとの平文コードに復元する復号手段と、

を備えて構成されることを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘匿対象となる平文コードに対し、ＰＮ（Pseud Noise:疑似雑音）信号との間で排他的論理和演算を行わせる暗号化を施すことにより、暗号コードを生成するストリーム暗号化方法の改良に関する。

【０００２】

【従来の技術】

現代は高度情報化社会といわれているが、真に公平で公正な社会システムを築いていくには、情報の通信・保存の場面で秘匿性が頑健に保たれていることが必須である。

【０００３】

こうした要請に応える仕組みのひとつが、情報の通信・保存の場面で秘匿性を担保する情報の暗号化である。アナログ暗号における情報の秘匿性は高い。しかし、その技術的な取り扱いは極めて煩雑であり、ほとんど実用化されていない。ディジタルコンピュータの発展とあいまって、ディジタルファイルをディジタル的に暗号化する方法が、現在のところ主流となっている。

【０００４】

そうしたディジタル暗号化方法のひとつとして、従来より、秘匿対象となる平文コードを個々の文字単位で逐次取り出し、こうして逐次取り出した平文コードの構成ビットに対し、ＰＮ信号の構成ビットとの間で排他的論理和演算を順次行わせる暗号化を施すことにより、暗号コードを生成するストリーム暗号化方法が一般に知られている。

【０００５】

こうしたストリーム暗号化方法を採用することで、情報への不正なアクセスを防止し、正当なアクセスのみを保証しようとしている。

【０００６】

【発明が解決しようとする課題】

ところで、上述した従来のストリーム暗号化方法では、暗号強度のさらなる向上を企図して、平文コードのデータ量と暗号コードのデータ量との対応関係を一対多とする、いわゆる拡散と呼ばれる手法が一般に多用されている。しかし、こうした拡散による暗号強化アプローチでは、平文コードのデータ量と比較して、拡散倍率の分だけ暗号コードのデータ量が膨張してしまい、ひいては通信負荷の増大を招くことにもなりかねない。このように、暗号強度の向上と、通信負荷の増大抑制とは、相反するトレードオフの関係に立つ訳であるが、こうした関係を踏まえた上で、前記両要望を可及的に満足することができるストリーム暗号化方法の開発が待望されていた。

【０００７】

本発明は、上述した背景技術に鑑みてなされたものであり、ストリーム暗号化方法において主要な役割を果たすＰＮ信号の周期として、平文コードの処理基本単位とは相容れない周期を採用することにより、暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能なストリーム暗号化方法を提供することを課題とする。

【０００８】

また、本発明は、上述したストリーム暗号化方法を用いて暗号化された暗号コードを、もとの平文コードに復元する用途に用いて最適な復号方法を提供することを課題とする。

【０００９】

そして、本発明は、上述したストリーム暗号化方法を用いて情報の暗号化を行う一方、上述した復号方法を用いて暗号コードをもとの平文コードに復元することにより、送信側と受信側との間で情報の暗号通信を実行可能に構成された暗号通信システムを提供することを課題とする。

【００１０】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の発明は、秘匿対象となる平文コードに対し、ＰＮ信号との間で排他的論理和演算を行わせることにより、暗号コードを生成するストリーム暗号化方法において、前記ＰＮ信号の周期として、前記平文コードの処理基本単位とは相容れない周期を採用したことを要旨とする。

【００１１】

請求項１の発明では、ＰＮ信号の周期として、平文コードの処理基本単位とは相容れない周期を採用している。そうした構成を採用することにより、暗号コードを構成する符号列は非常によくかき混ぜられるので、暗号コードを通じて原文が透けて見えることを防ぐという意味で、きわめて優れた効果を発揮する。

【００１２】

これについて述べると、ストリーム暗号化方法では、ＰＮ信号は暗号鍵に相当する。一般に、暗号鍵の種類が多いほど、換言すれば、ＰＮ信号の周期、つまりそのビット長が長いほど、システムの頑健性は向上する。しかし、暗号鍵の管理と、不正アクセス防止のための照合の便宜を考えた場合、あまりに長いＰＮ信号では扱いにくい。そこで、ＰＮ信号の周期について、単なる長短の調整とは異なる視点での技術的アプローチによって、暗号コードを通じて原文が透けて見えることを防止できれば、本発明の所期の目的を達成することができることになる。その答えは、ＰＮ信号の周期として、平文コードの処理基本単位とは相容れない周期を採用することにある。具体的には、例えば、平文コードの処理基本単位を８ビット（偶数）と仮定したとき、この８ビット（偶数）とは相容れないＰＮ信号の周期として、２３ビット（奇数）を採用するようにする。この場合、８ビットと２３ビットとは、相互の先頭ビットが同期している時間軸上の部分から起算して、最小公倍数たる８＊２３＝１８４ビット周期目ではじめて同期がとれる。このように、相互同期のための周期が比較的長くなるような、平文コードの処理基本単位と、ＰＮ信号の周期と、の組み合わせに係る周期を、相容れない周期と呼んでいる。こうした工夫を施すことにより、暗号コードを構成する符号列はきわめてよくかき混ぜられる結果として、暗号コードを通じて文字や数値などの原文が透けて見えるのを効果的に予防することができる。

【００１３】

請求項１の発明によれば、ＰＮ信号の周期について、単なる長短の調整とは全く異なり、平文コードの処理基本単位との非親和性確保という視点での周期調整を内容とする技術的アプローチによって、暗号コードを通じて原文が透けて見えることを防止するようにしたので、暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能なストリーム暗号化方法を提供することができる。

【００１４】

また、請求項１の発明によれば、本発明が独立してある程度の暗号強度の向上効果を期待し得る結果として、例えば、ＰＮ信号として比較的短い周期を採用した場合には、拡散によってデータ量を膨張させない、平文コードと暗号コードとの各データ量が一対一で対応付けられる直接暗号化についての可能性を拡げ、通信負荷の増大抑制といった付随的な効果を奏する一方で、ＰＮ信号として比較的長い周期を採用した場合には、それ自体による暗号強度向上効果と、本発明独自での暗号強度向上効果と、があいまって、きわめて優れた暗号強度向上効果を奏するであろうことを期待することができる。

【００１５】

ところで、暗号化を行う上で重要な役割を果たすＰＮ信号としては、例えば、従来公知の擬似乱数生成法を用いて２進コード列を生成し、生成した２進コード列のなかから、本発明の所期の目的達成に適した所要のビット長だけ切り出した信号列を採用することができる。また、ＰＮ信号としては、上述した形態に限定されることなく、例えば、カオスを生成する一次元写像回路のＣＭＯＳスイッチを介したフリップフロップループの出力を、１ビット量子化器（ＡＤ変換器）を通して二値符号化した２進コード列から適宜のビット長となる符号列を切り出して利用することができる。さらに、初期値からのカオス系列をそのままＰＮ信号の周期信号として利用してもよい。さらにまた、工業用汎用ＣＰＵや汎用ディジタルコンピュータに、

ロジスティックマップ関数　$x(t+1)=4x(t)\{1-x(t)\}$、

フィードバック　$x(t)=x(t+1)$、

同相変換量子化　$y(t)=[2/\pi \cdot \arcsin\sqrt{x(t)} \cdot 2^n]=[2x(t)]'$　(n=1のとき、[]は小数点以下を切り捨てる)

を計算させ、得られた２進コード列から適宜のビット長となる符号列を切り取ってＰＮ信号としてもよい。

【００１６】

請求項１の発明では、ＰＮ信号の周期についての選び方に特徴を有するストリーム暗号化方法について述べたが、この方法を用いて暗号化した暗号コードを、どのようにしてもとの平文コードに復元するか、が問題となる。

【００１７】

そうした観点から、請求項２の発明は、請求項１に記載のストリーム暗号化方法を用いて暗号化された暗号コードを平文コードに復元する復号方法において、前記暗号コードに対し、前記ＰＮ信号と同一のＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、前記暗号コードをもとの平文コードに復元することを要旨とする。

【００１８】

請求項２の発明では、暗号コードに対し、前述のＰＮ信号と同一のＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、暗号コードをもとの平文コードに復元する。具体的には、暗号コードの復元に際しては、暗号コードとＰＮ信号との再度の排他的論理和演算を、同期をとって実行する。暗号コードに対してＰＮ信号が非同期のときには、暗号コードはもとの平文コードの通り正しく復元されずに、単なる雑音信号となってしまう。

【００１９】

請求項２の発明によれば、ＰＮ信号の周期に関する選び方に特徴を有するストリーム暗号化方法を用いて暗号化した暗号コードを、もとの平文コードに復元するための手順を提供することができる。

【００２０】

そして、請求項３の発明は、図１に示すように、送信側と受信側との間で情報の暗号通信を遂行し得るように構成された暗号通信システム１１において、前記送信側は、秘匿対象となる平文コードを処理基本単位毎に記憶する平文記憶手段

１３と、前記平文コードの処理基本単位とは相容れない周期となるＰＮ信号を記憶する送信側ＰＮ信号記憶手段１５と、前記平文記憶手段１３に記憶されている平文コードに対し、前記送信側ＰＮ信号記憶手段１５に記憶されているＰＮ信号との間で排他的論理和演算を行わせることにより、暗号コードを生成する暗号化手段１７と、この暗号化手段１７で生成した暗号コードを受信側宛に送信する送信手段１９と、を備える一方、前記受信側は、前記送信手段１９から送信されてきた暗号コードを受信する受信手段２１と、この受信手段２１で受信した暗号コードを処理基本単位毎に記憶する暗号文記憶手段２３と、前記送信側ＰＮ信号記憶手段１５に記憶されているＰＮ信号と同一のＰＮ信号を記憶する受信側ＰＮ信号記憶手段２５と、前記暗号文記憶手段２３に記憶されている暗号コードに対し、前記受信側ＰＮ信号記憶手段２５に記憶されているＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、前記暗号コードをもとの平文コードに復元する復号手段２７と、を備えて構成されることを要旨とする。

【００２１】

請求項３の発明に係る暗号通信システム１１では、図１に示すように、まず、送信側において、暗号化手段１７は、平文記憶手段１３に記憶されている平文コードに対し、送信側ＰＮ信号記憶手段１５に記憶されているＰＮ信号との間で排他的論理和演算を行わせることにより、暗号コードを生成する。これを受けて、送信手段１９は、暗号化手段１７で生成された暗号コードを、受信側宛に送信する。一方、受信側において、受信手段２１は、送信手段１９から送信されてきた暗号コードを受信する。これを受けて、暗号文記憶手段２３は、受信手段２１で受信された暗号コードを処理基本単位毎に記憶する。そして、復号手段２７は、暗号文記憶手段２３に記憶されている暗号コードに対し、受信側ＰＮ信号記憶手段２５に記憶されている、送信側ＰＮ信号記憶手段１５のＰＮ信号と同一のＰＮ信号との間で同期をとって排他的論理和演算を行わせることにより、暗号コードをもとの平文コードに復元する。

【００２２】

請求項３の発明によれば、送信側では、ＰＮ信号の周期に関する選び方に特徴を有するストリーム暗号化方法を用いて暗号化した暗号コードを送信する一方、

受信側では、上述した手順で暗号化された暗号コードを、再度の排他的論理和演算を行わせることでもとの平文コードに復元するようにしたので、暗号コードを構成する符号列は非常によくかき混ぜられる結果として、暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能な暗号通信システムを得ることができる。

【００２３】

【発明の実施の形態】

以下に、本発明に係るストリーム暗号化方法、復号方法、及び暗号通信システムの実施形態について、図２乃至図３を参照して説明する。

【００２４】

図２乃至図３は、本発明に係るストリーム暗号化方法が奏する暗号強度の向上度合いの説明に供する図である。

【００２５】

文字や数字などを表現するための文字体系のうち、例えばアスキーコードでは、７ビットで９６個の大小英文字、数字、特殊文字と３２個の制御文字を含めて都合１２８個の文字を表現できる。この場合、今日のデジタルコンピュータにおける情報の処理基本単位たる８ビット（１バイト）のうち、先頭ビットが常に０になっている。このことから、アスキーコードそれ自体の出現頻度分布では、８ビット（0～255）のうち前半部分（0～127）にしか分布せず、残りの後半半分（128～255）には分布し得ないことになる。

【００２６】

図３はＰＮ信号のビット長Ｌとして２４ビットを用い、アスキーコードで表現される英文ファイルを、平文コードと暗号コードとの各データ量が一対一で対応付けられるようにストリーム暗号化し、その暗号コードの出現頻度分布を表した結果である。分布は左半分に片寄っている。左半分の中ではかなりよく混ぜ合わされているが、原文が英文であることを第三者から容易に推察されてしまう。

【００２７】

図２はＰＮ信号のビット長Ｌとして２３ビットを用い、図１と同様にアスキーコードで表現される英文ファイルを、平文コードと暗号コードとの各データ量が

一対一で対応付けられるようにストリーム暗号化し、その暗号コードの出現頻度分布を表した結果である。暗号コードは８ビット（0～255）全体にわたり拡散・混合されている。もはや暗号コードの出現頻度分布から、原文が英文か和文か、または数値データであったのか、などを第三者が推察することは到底不可能である。

【００２８】

なお、こうしたＰＮ信号のビット長Ｌ＝｛２３，２４｝の組合わせに係る比較は単なる一例に過ぎない。すなわち、例えば、ビット長Ｌ＝｛７，８｝、｛１５，１６｝、｛６３，６４｝などの組合わせに係る比較実験おいても、暗号コードの混合効果として顕著な差異がみられる。

【００２９】

ＰＮ信号のビット長Ｌ＝２３ビットでは、Ｌ＝２４ビットとは単なる１ビットのビット長の相違にしか過ぎないが、暗号コードの頑健性の観点からは、図１と図２の比較から明らかなように、顕著な相違がみられる。

【００３０】

このように、一般に８ビット長が多用される情報の処理基本単位とは相容れないビット長を周期とするＰＮ信号の採用が、情報通信や情報保存の社会的安全性を飛躍的に向上させ得ることはまさに注目すべきことであろう。

【００３１】

なお、上述した実施の形態は、本発明の理解を容易にするために例示的に記載したものであり、本発明の技術的範囲を限定するために記載したものではない。したがって、本発明は、その技術的範囲に属する全ての実施の形態を含むことは当然として、そのいかなる均等物をも含む趣旨である。

【００３２】

すなわち、例えば、本実施の形態中、平文コードの符号体系として、アスキーコードを例示して説明したが、本発明はこの形態のみに限定されることなく、ＩＳＯ符号、ＥＢＣＤＩＣ符号、ＪＩＳ符号、または漢字ＪＩＳ符号などを含む符号体系を適宜採用することができることは言うまでもない。

【００３３】

【発明の効果】

以上詳細に説明したように、請求項１の発明によれば、ＰＮ信号の周期について、単なる長短の調整とは全く異なり、平文コードの処理基本単位との非親和性確保という視点での周期調整を内容とする技術的アプローチによって、暗号コードを通じて原文が透けて見えることを防止するようにしたので、暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能なストリーム暗号化方法を提供することができる。

【００３４】

また、請求項１の発明によれば、本発明が独立してある程度の暗号強度の向上効果を期待し得る結果として、例えば、ＰＮ信号として比較的短い周期を採用した場合には、拡散によってデータ量を膨張させない、平文コードと暗号コードとの各データ量が一対一で対応付けられる直接暗号化についての可能性を拡げ、通信負荷の増大抑制といった付随的な効果を奏する一方で、ＰＮ信号として比較的長い周期を採用した場合には、それ自体による暗号強度向上効果と、本発明独自での暗号強度向上効果と、があいまって、きわめて優れた暗号強度向上効果を奏するであろうことを期待することができる。

【００３５】

請求項２の発明によれば、ＰＮ信号の周期に関する選び方に特徴を有するストリーム暗号化方法を用いて暗号化した暗号コードを、もとの平文コードに復元するための手順を提供することができる。

【００３６】

そして、請求項３の発明によれば、送信側では、ＰＮ信号の周期に関する選び方に特徴を有するストリーム暗号化方法を用いて暗号化した暗号コードを送信する一方、受信側では、上述した手順で暗号化された暗号コードを、再度の排他的論理和演算を行わせることでもとの平文コードに復元するようにしたので、暗号コードを構成する符号列は非常によくかき混ぜられる結果として、暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能な暗号通信システムを得ることができるというきわめて優れた効果を奏する。

【図面の簡単な説明】

【図１】

図１は、本発明に係る暗号通信システムの機能ブロック構成図である。

【図２】

図２は、本発明に係るストリーム暗号化方法が発揮する効果の説明に供する図である。

【図３】

図３は、本発明に係るストリーム暗号化方法が発揮する効果の説明に供する図である。

【符号の説明】

１１　暗号通信システム

１３　平文記憶手段

１５　送信側ＰＮ信号記憶手段

１７　暗号化手段

１９　送信手段

２１　受信手段

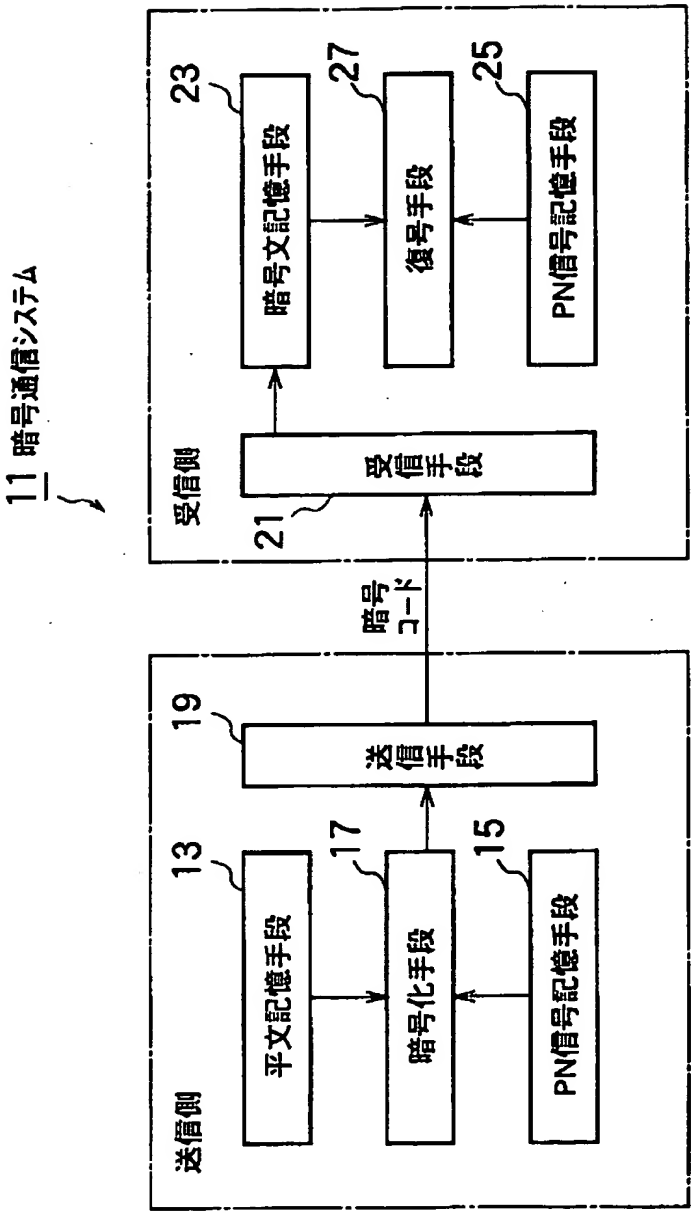
２３　暗号文記憶手段

２５　受信側ＰＮ信号記憶手段

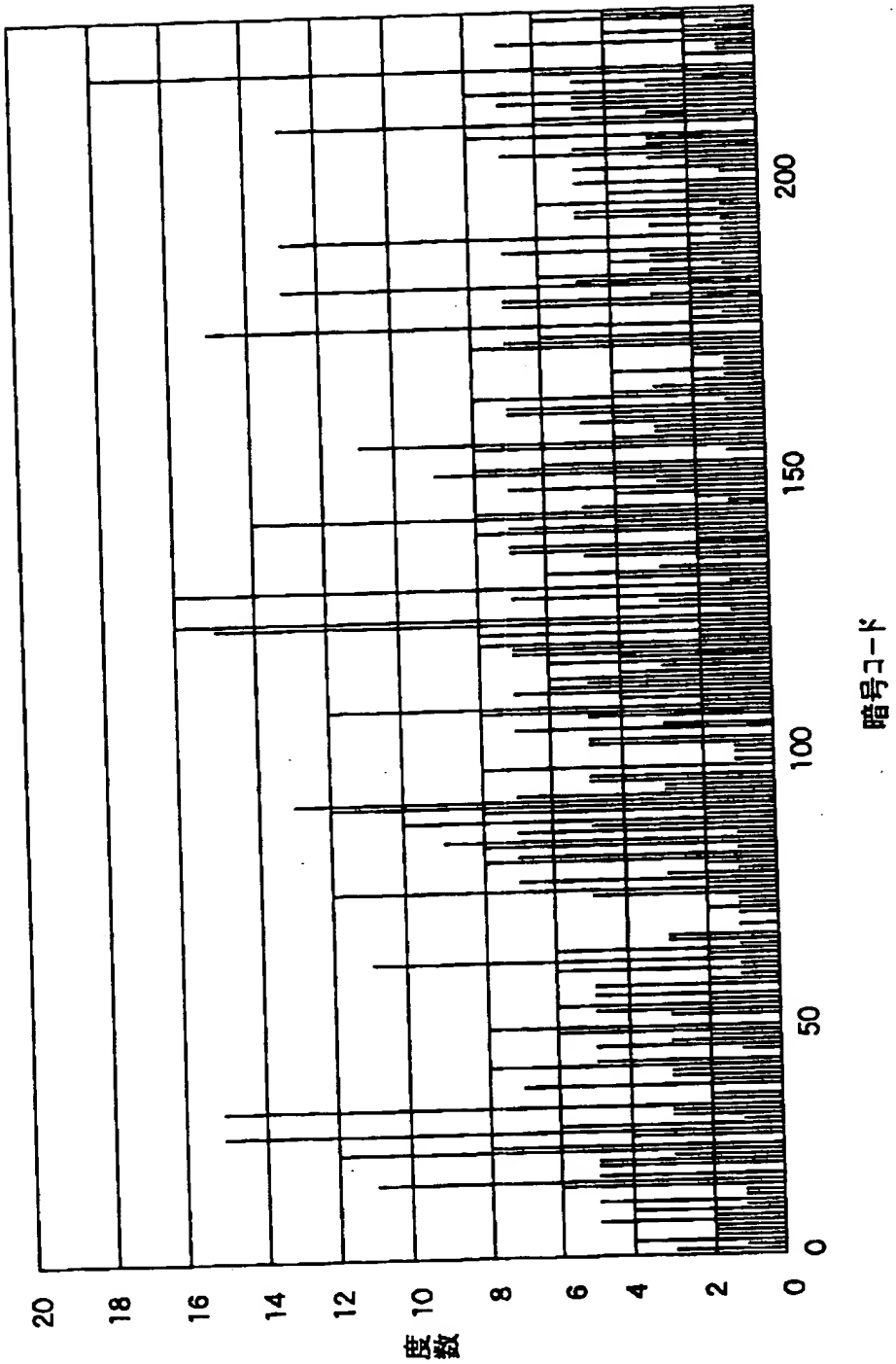
２７　復号手段

【書類名】　　図面

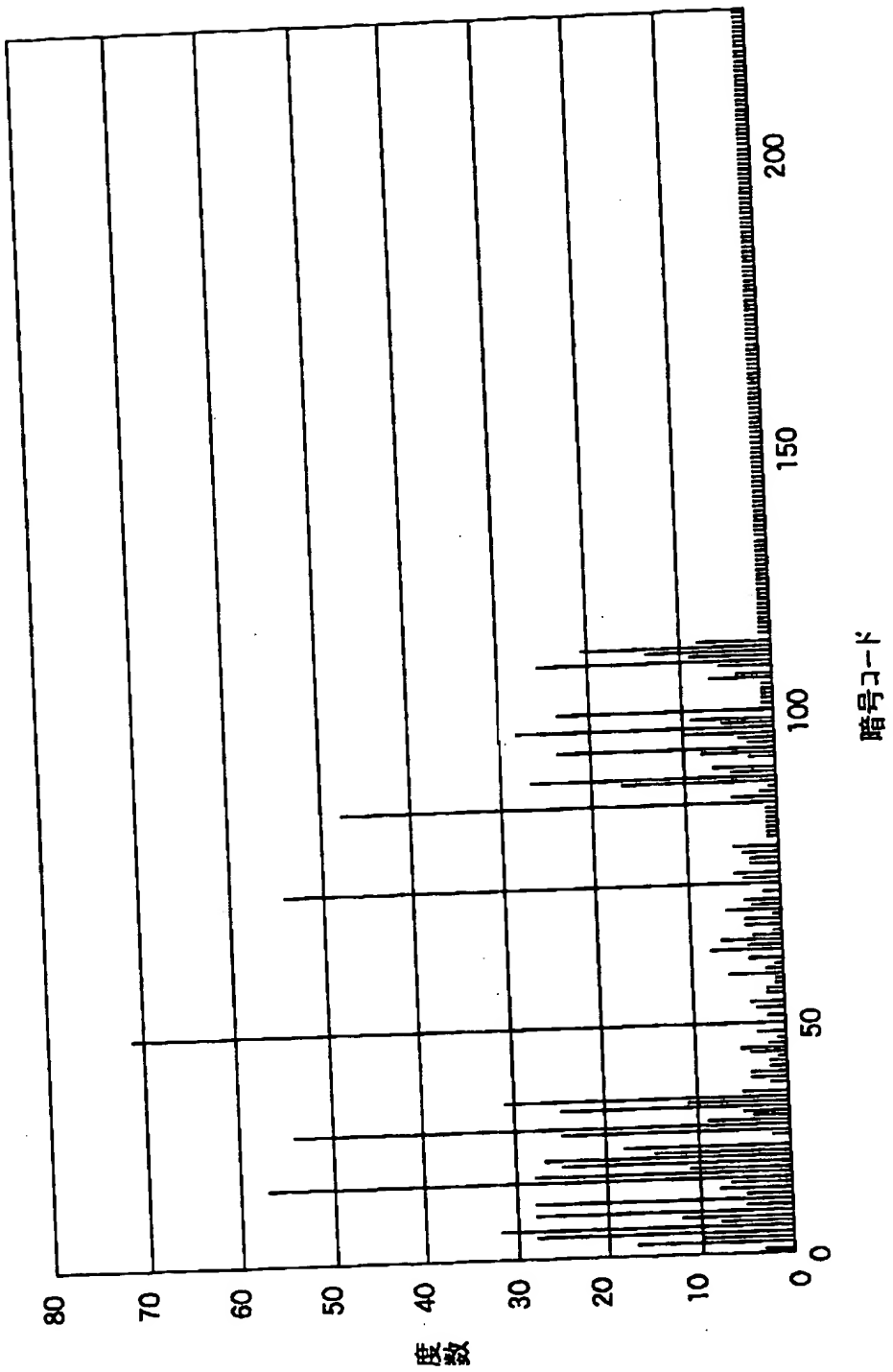
【図１】


11 暗号通信システム
受信側
23
暗号文記憶手段
27
復号手段
25
PN信号記憶手段
受信手段
21
暗号コード
送信側
19
送信手段
13
平文記憶手段
17
暗号化手段
15
PN信号記憶手段

【図２】



【図３】



【書類名】　　要約書

【要約】

【課題】　暗号強度の向上と、通信負荷の増大抑制と、の両要望を可及的に満足することが可能なストリーム暗号化方法、復号方法、及び暗号通信システムを提供することを課題とする。

【解決手段】　送信側において、暗号化手段１７は、ＰＮ信号の周期に関する選び方に特徴を有するストリーム暗号化方法を用いて平文コードを暗号化し、これを受けて送信手段１９は、前記暗号化された暗号コードを送信する一方、受信側において、復号手段２７は、上述した手順で暗号化された暗号コードを、再度の排他的論理和演算を行わせることでもとの平文コードに復元するようにした。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００６８９５〕

１．変更年月日　１９９０年　９月　６日
［変更理由］　新規登録
住　所　東京都港区三田１丁目４番２８号
氏　名　矢崎総業株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９１２３５８１０〕

１．変更年月日　　１９９４年　４月１２日
［変更理由］　住所変更
住　所　　東京都文京区大塚６丁目７番４－３０２号
氏　名　　マイクロテクノロジ株式会社